

Application No. 09/761,373
Amendment "A" dated November 4, 2004
Reply to Office Action mailed August 23, 2004

REMARKS

The first Office Action, mailed August 23, 2004, considered and rejected claims 1-35 in view of Jones (U.S. Patent No. 5,412,730), Thompson (U.S. Patent No. 6,357,046) and Patel (U.S. Patent No. 6,327,660).¹

By this paper, claims 1, 13, 15, 23, 33 and 35 have been amended and claims 4, 17 and 25 have been cancelled, such that claims 1-3, 5-16, 18-24, 26-35 remain pending, of which claims 1, 13, 15, 23, 33 and 35 are the only independent claims that remain at issue.

As discussed during the interview, the pending claims are generally directed to embodiments for encrypting data to guard against eavesdropping and brute force attacks. According to the present invention, a master secret is negotiated between two computing systems. Next, a random seed is generated for each data packet to be delivered from a transmitting computer to a recipient computer. A different random seed is created for each data packet through the use of a random bit sequence that is created for each data packet. The master secret and different random seed of each data packet is then applied to a key generation module to generate a corresponding key for each data packet and in such a way that a different key is created for each data packet. The data packet is then encrypted with the key and transmitted with the seed to the recipient computer as a data structure.

The recipient computer then inputs the transmitted/received seed of each data packet, along with the pre-negotiated master secret into a key generation module to generate the key that

¹ Claims 1-2, 4, 7-8, 10-17, 21-23, 25, 28-29 and 31-35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Thompson. Claims 3, 5-6, 9, 18-20, 24, 26-27 and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jones in view of Thompson and further in view of Patel. Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

Application No. 09/761,373
Amendment "A" dated November 4, 2004
Reply in Office Action mailed August 23, 2004

was used to encrypt the data packet. This key is then used to decrypt each corresponding data packet.

The independent claims are directed to various perspectives of the aforementioned invention. For example, claims 1, 13 and 15 are drafted from the perspective of the transmitting/encrypting computer, whereas claims 23 and 33 are directed from the perspective of the receiving/decrypting computer, and whereas claim 35 is directed to a system that includes both of the computers.

As discussed during the interview, the cited art fails to anticipate or obviate the foregoing claims. In particular, the cited art fails to disclose or suggest any method wherein a different random seed is generated for each data packet to be encrypted and transmitted between the computers.

For example, as recited in Jones, "Once the host station has supplied the initial seed value keys to the units forming the two terminal locations for a given link and transmission over that link begins, the host is no longer "knows" the encryption key values since they are dependent upon the nature of the transmissions over the link. Consequently, link security cannot be compromised even by an "insider" who is in possession of the initial key values supplied by the host." Col. 2, ll. 17-25. Accordingly, "In accordance with a principle feature of the present invention, pseudo-random number generators are employed at both the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without those keys being transmitted in any form over the transmission facility." Col. 1, ll. 37-42. For at least those reasons, as well as the others disclosed during the interview, Jones fails to disclose or suggest the embodiments recited in the pending claims.

Application No. 09/761,373
Amendment "A" dated November 4, 2004
Reply to Office Action mailed August 23, 2004

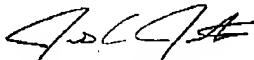
As further discussed during the interview, the other cited art also fails to disclose or suggest any method, as recited in the pending claims, wherein a different random seed is generated for each data packet to be encrypted and transmitted between the computers in combination with the other recited claim elements.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that the pending claims are neither anticipated by nor obviated by the art of record, and are now therefore in condition for allowance.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 4 day of November 2004.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant

Customer No. 47973

RDN:JCJ:cm
W:\13768\191\CM\000004336V001.DOC